

REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Claim 1-9 are pending.

The examiner again rejects claims 1-9 under 35 U.S.C. Sec. 103 as obvious over McDonnal.

McDonnal discloses a technique for selecting one of files stored in a memory, and decrypting data of the file and automatically deleting the decrypted data. In the disclosed system, if at the time the file is automatically deleted, the decrypted data has not been modified, then the decrypted data is just scorched and no reencryption of the decrypted data is performed, while if the decrypted data has been modified, then reencryption of the decrypted data is performed prior to the scorching of the decrypted data so as to make an encrypted copy of the to-be scorched modified data (refer to claim 3 of McDonnal). That is, the criterion (for determining the operation) is "whether the decrypted data has been modified", and based on the criterion, one of (i) deleting of the file and (ii) reencryption of the file is chosen. In contrast, in the claimed invention, the criterion (for determining the operation) is "whether an illegal try (i.e., an illegal access to the system) is performed", and based on this criterion, one of (i) providing the same key for a cryptosystem key used for reencrypting the secret information and a cryptosystem key which is stored as the updated cryptosystem key and (ii) providing different keys for the above two kinds of cryptosystem keys is chosen. That is, the criterion and the operation based on the criterion each differ from those of the system of McDonnal.

Additionally, in the claimed invention, when an illegal try has been detected, the updated key used for reencryption is not stored and a different key is instead stored. According to this distinctive feature, the reencrypted data (i.e., reencrypted when an illegal try has been detected) cannot be decrypted by any means. It is

submitted that such distinctive features are not made obvious by McDonnal or any other prior art.

Furthermore, in the present invention, the secret information itself is not deleted in any case, and reencryption is always performed and the reencrypted data is stored. That is, the secret information is not deleted and is reencrypted regardless of the results of determination based on the above-explained criterion. Therefore, the secret information itself is always present. Accordingly, an illegal user may try to decrypt the secret information by using an incorrect key and believe that the decrypted secret information can be obtained, in spite of the fact that the decrypted information is incorrect. Therefore, the present invention also has an effect of deceiving the illegal user. Accordingly, the present invention clearly differs from McDonnal with respect to the criterion for determination and the function (or operation).

The current amendments to the claims were prompted by the examiner's comments in the outstanding office action under the section "Response to Amendment" in which the examiner faulted applicant's preamble for not including the recitation of the cryptosystem key updating (method or system). This amendment is intended to cure such perceived defect. The title of the invention has also been changed accordingly. It is submitted that the amendments do not raise new issues because the cryptosystem limitations were already recited in all of applicant's claims and the additional recitation in the preamble is made for emphasis only and to respond to the examiner's comments.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741.

If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date December 8, 2003

FOLEY & LARDNER
Customer Number: 22428
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By 

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257